(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 063 812 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
19.07.2006 Bulletin 2006/29

(51) Int Cl.:
H04L 9/08 *(2006.01)* ***H04L 9/32*** *(2006.01)*

(21) Application number: **00304560.6**

(22) Date of filing: **30.05.2000**

(54) **Methods and equipment for encrypting/decrypting, and indentification systems**

Verfahren und Vorrichtung zur Verschlüsselung/Entschlüsselung sowie Identifikationssysteme

Procédés et dispositif de chiffrage/déchiffrage et systèmes d'identification

(84) Designated Contracting States:
DE FR GB

(30) Priority: **21.06.1999 JP 17464899**

(43) Date of publication of application:
27.12.2000 Bulletin 2000/52

(60) Divisional application:
05008651.1 / 1 557 971
05008652.9 / 1 562 319

(73) Proprietor: **FUJITSU LIMITED**
Kawasaki-shi,
Kanagawa 211-8588 (JP)

(72) Inventors:
- **Fujii, Yusaku**
  c/o Fujitsu Limited
  Kawasaki-shi,
  Kanagawa 211-8588 (JP)
- **Shinzaki, Takashi**
  c/o Fujitsu Limited
  Kawasaki-shi,
  Kanagawa 211-8588 (JP)

(74) Representative: **Wilding, Frances Ward et al**
HASELTINE LAKE
Imperial House
15-19 Kingsway
London WC2B 6UD (GB)

(56) References cited:
WO-A-98/29983
WO-A-98/48538
GB-A- 2 331 825
US-A- 4 993 068
US-A- 5 737 420
US-A- 5 790 668

EP 1 063 812 B1

Description

[0001] The present invention relates to encryption/decryption methods and equipment adapted for physical characteristic information such as fingerprints, voiceprints, palm patterns, facial appearances, or signatures or signatures representing a characteristic inherent to an individual, and to remote identification systems for identifying a person through a network according to the physical characteristic information.

[0002] The fingerprints, voiceprint, iris patterns or the like are characteristics inherent to an individual and are invariable for the life of the individual so that they are excellent as information for identifying a person and are utilized in various identification systems such as an admission controlling system.

[0003] As an information-related device such as a personal computer spreads, on the other hand, a variety of information are vigorously sent and received through a network between end users to enhance the importance of commerce through the network and transmissions of documents.

[0004] In order to perform the commerce and the exchanges of important documents properly through the network, there has been needed a technique for sending and receiving information to prove each other through the network and for identifying the persons reliably between each other. So the physical characteristic information has been noted as the information for identifying the persons.

[0005] Fig. 1 of the accompanying drawings is a diagram showing a construction of a remote identification system of the prior art through a network.

[0006] The remote identification system shown in Fig. 1 is constructed such that a client-side identification equipment 410 sends authenticating information through the network, and such that a server-side identification equipment 420 identifies the person of the client-side identification equipment 410, according to the result of comparison between the received authenticating information and the registered authenticating information.

[0007] When a personal computer communication service is utilized, for example, the end user's personal computer is the client-side identification equipment, and the host computer of a service provider is the server-side identification equipment.

[0008] In this case, according to a user's ID and a password inputted through a keyboard 411, the authenticating information is generated by a request controlling part 412 and is sent to the network by a transmission controlling part 413.

[0009] At this time, the aforementioned password is encrypted by an encrypting part 414, and this encrypted password is used in the request controlling part 412 to generate the authenticating information so that the password can be safely transferredthrough the network to the server-side identification equipment 420.

[0010] In the server-side identification equipment 420 shown in Fig. 1, the aforementioned encrypted password is received by a transmission controlling part 422 and transferred to a decrypting part 421. Accordingly, the decrypting part 421 decrypts the encrypted password and transfers the password to an identification controlling part 423.

[0011] On the other hand, the aforementioned user' s ID is received by the transmission controlling part 422 and then transferred to the identification controlling part 423. According to this user's ID, the identification controlling part 423 retrieves the registered password from a password data base 424, and compares this password with the password restored by the decrypting part 421.

[0012] In this case, if the restored password and the registered password match each other, the identification result having confirmed the identity is informed to the client-side identification equipment 410 by the transmission controlling part 422. Accordingly, the request controlling part 412 generates a message indicating the identification result and informs the person of the fact that the permission was acknowledged, by a display (CRT) 415.

[0013] As shown in Fig. 1, on the other hand, the encrypting part 414 may encrypt the password by using the current time on the system, as received from the digital timing unit 416, and the decrypting part 421 may decrypt the encrypted password by using the current time on the system, as received from a digital timing unit 425.

[0014] In this case, the password inputted by the person can be converted into a different cryptogram each time so that it can be safely sent and received through the network.

[0015] In this remote identification system, the inputted password is the information for identifying the person so that the password has to be properly managed by each person so as to identify the person reliably to exclude others.

[0016] On the other hand, the physical characteristic information is inherent to an individual and is excellent as one for the identification so that it is utilized as the authenticating information for the persons in the admission controlling system, for example.

[0017] Fig. 2 is a diagram showing an example of the construction of the identification system utilizing the physical characteristic information.

[0018] Fig. 2 shows the case in which the information representing a feature of a fingerprint is used as the physical characteristic information. This identification system is constructed to include a fingerprint reader 430 and fingerprint identification equipment 440.

[0019] In this identification system, the fingerprint reader 430 acquires the information featuring the fingerprint of a person being present at the site as a series of numeric data and inputs the aforementioned information to the fingerprint identification equipment 440 through an identification controlling part 401.

[0020] A set of numeric data representing the feature of a fingerprint will be referred to as the "fingerprint data".

[0021] In the fingerprint reader 430 shown in Fig. 2, a

feature extracting part 431 receives the image data read by an image inputting part 432, and extracts the feature of the fingerprint appearing in that image.

[0022] The features, as extracted by the feature extracting part 431, are arrayed according to a predetermined format by a fingerprint data generating part 433, and the fingerprint data thus generated are transferred to the identification controlling part 401.

[0023] In the fingerprint identification equipment 440 shown in Fig. 2, a fingerprint database 441 is registered with the user's ID given to an individual having an admission and fingerprint data (hereunder referred to as "reference data") obtained by measuring the related individuals. On the other hand, the user' s ID inputted from a keyboard 402 is transferred to a fingerprint data retrieving part 442 by the identification controlling part 401, so that the related fingerprint data are retrieved from the aforementioned fingerprint database 411 by the fingerprint data retrieving part 442 based on that user's ID and subjected to the processing of a verifying part 444.

[0024] Here, the numeric data obtained by measuring the physical characteristic information including fingerprints generally fluctuate at each measurement by the condition for the measurement.

[0025] By the pressure to be applied to a finger when the finger is pushed to the image inputting part 432, the temperature of the finger or the ambient humidity, for example, the image data to be read change in a subtle way. Accordingly, the patterns of ridge flows in an image of the fingerprint and the distributions of the ridge points or the ridge bifurcations fluctuate.

[0026] According to the recognition rate required, therefore, the verifying part 444 decides whether or not the inputted fingerprint data belong to the eligible person, depending upon whether or not components in a predetermined area of the inputted fingerprint data are equivalent to the components in the corresponding area of the reference data.

[0027] Fig.3 is a diagram for explaining a processing for comparing the physical characteristic information.

[0028] For an application to allow a misidentification of about one to one hundred, for example, the verifying part 444 may compare a limited portion of the inputted fingerprint data with the reference data, as illustrated as a observing area in Fig. 3A, and may inform the identification controlling part 401 whether or not the variance of all the components contained in the observing area is within a predetermined allowable range.

[0029] If the variance between the individual components of the reference data and the individual components of the inputted fingerprint data is within the allowable range in the hatched area of Fig. 3A, for example, the verifying part 444 informs the identification controlling part 401 of the fact that the inputted fingerprint data and the reference data are equivalent.

[0030] In response to this, the identification controlling part 401 may identify the person, have a displaying part 403 display that the person is admitted, and perform the necessary controls such as unlocking the door by utilizing the function of the admission controlling part 404.

[0031] If the variance of a portion of the component included in the aforementioned observing area exceeds the allowable range, as illustrated in Fig. 3B, the verifying part 444 may inform that the reference data and the inputted fingerprint data are not equivalent. In response to this, the identification controlling part 401 may perform the controls necessary for denying the admission of the person.

[0032] Here, if the fingerprint data are recognized by using the relatively narrow area as the observing area, as illustrated in Fig. 3A, a misidentification of about one to one hundred may occur, but the possibility of excluding the person can be lowered even if the condition for measuring the fingerprint data is poor.

[0033] For an application requiring a misidentification of about one to ten thousands, on the other hand, most of the fingerprint data has to be confined in the observing area, as illustrated in Fig. 3C.

[0034] In this case, the possibility of the misidentification can be lowered, but the possibility that even the person able to be admitted may be denied because of having slight dirtiness of the fingertip will rise. This is because the wider the observing area the larger the possibility that the variance between the individual components of the inputted fingerprint data and the individual components of the reference data may exceed the allowable range.

[0035] As the technique for transmitting the information safely through the network, there was already practiced the RSA algorithm for realizing the public key system or the DES (Data Encryption Standard) method applying the common key system.

[0036] The DES method is a cryptographic method for dividing the information to be encrypted into blocks of a unit of 64 bits and for converting the individual blocks by combining a substitution cipher and a transposition cipher complicatedly. The DES method is called the "block encryption" because the conversion unit is the block.

[0037] In the aforementioned remote identification system of the prior art, the password or the information for providing the identity is basically left to the management of an individual .

[0038] In order to block the plagiarism of the password, on the other hand, it is required that the password has a sufficient length, be a meaningless string of characters and be frequently changed. This makes it difficult for the individual to manage the password properly.

[0039] This is because a person finds it difficult to memorize the meaningless string of characters or symbols, and because the necessity of frequent change is too heavy a burden for the person.

[0040] As a matter of fact, most users register such passwords as can be easily analogized from the personal information being opened to the public or the kind of information to be preferably accessed to, record and carry the memorandum of the password or forget to change the password for a long time.

[0041] In the remote identification system using only the password as the information for identifying the person, therefore, it is difficult to ensure the safety necessary for the e-commerce or for sending and receiving the important information.

[0042] By introducing the remote identification system using the physical characteristic information inplace of the password as the information for the identification, it is possible to block fraudulent access. So important information can be sent and received safely through the network.

[0043] Fig. 4 shows an example of the construction of the remote identification system utilizing the physical characteristic information.

[0044] In the client-side identification equipment 410 shown in Fig. 4, the fingerprint data obtained by the fingerprint reader 430 are encrypted by the encrypting part 414, and the obtained cryptogram is sent in place of the password to the network by the transmission controlling part 413.

[0045] This cryptogram is received by the transmission controlling part 422 provided in the server-side identification equipment 420 and is then transferred to the decrypting part 421 by the identification controlling part 401. In response to this, the decrypting part 421 decrypts the aforementioned cryptogram to restore the original fingerprint data, which are transferred together with the user's ID to the fingerprint identification equipment 440.

[0046] Premising that the physical characteristic information contains fluctuations and noises, when exactly the same physical characteristic information as the previously inputted one is inputted, that physical characteristic information is judged to have been plagiarized. Then, the attack using the plagiarized authenticating information can be blocked, making it possible to send and receive the information more safely.

[0047] The attack to break the protection of the remote identification system by using the plagiarized authenticating information will be referred to as "replay attack".

[0048] Here will be described an example of the remote identification system considering that replay attack.

[0049] In the remote identification system shown in Fig. 4, the replay attack is partially blocked by storing the fingerprint database 441 with not only the reference data related to each user's ID but also the registered fingerprint data that is previously inputted, by comparing the inputted fingerprint data with the reference data and the registered fingerprint data by a comparing part 445 provided in a verifying part 444, and by subjecting the result of comparison to the processings of a fraud detecting part 446 and of a recognizing deciding part 447.

[0050] Here, according to the comparison result received from the comparing part 445, the fraud detecting part 446 shown in Fig. 4 decides whether or not all the numeric data comprising the inputted fingerprint data and the corresponding numeric data of the reference data or the registered fingerprint data completely match, and informs, if they match, the recognizing deciding part 447 of the detection of the replay attack.

[0051] According to the comparison result received from the comparing part 445, on the other hand, the recognizing deciding part 447 decides whether or not the variance between the individual components of the inputted fingerprint data and the individual components of the reference data is within a predetermined allowable range, and further whether or not the inputted fingerprint data belong to the eligible person, according to the decision result and the detection result of the fraud detecting part 446, and informs this result of decision as the result of recognition to the identification controlling part 401.

[0052] In this case, it is conditions necessary for identifying a person that the inputted fingerprint data are equivalent to the reference data over the area covering the observing area, as illustrated in Fig. 4, and that all the numeric data comprising the inputted fingerprint data are not completely equal to the corresponding numeric data contained in the reference data or the registered fingerprint data.

[0053] Here, the cryptographic technique of the prior art, as represented by the aforementioned DES method, regards the difficulty at the time of restoring the original information from the cryptogram as important, and converts the original information by a complicated cryptographic algorithm. This makes it seriously difficult to decrypt the encrypted physical characteristic information to obtain the original physical characteristic information.

[0054] Since the physical characteristic information itself is inherent to each person, on the other hand, the information is extremely difficult to plagiarize or forge so long as it is properly managed.

[0055] Since the process for the encrypted physical characteristic information to be transmitted through the network has almost no protection, however, it is relatively easy to acquire that information fraudulently.

[0056] When the encrypted physical characteristic information fraudulently acquired by the wiretapping method or the like is utilized as it is, it can naturally be excluded as the replay attack, as has been described above.

[0057] When the fraudulently acquired encrypted physical characteristic information is partially altered, however, the decrypted physical characteristic information may satisfy the conditions necessary for identification described above by the influence of the alteration upon the decrypted physical characteristic information.

[0058] Because the fingerprint data having been encrypted by the aforementionedencrypting part 414 using the blockencrypting method such as the DES method are decrypted for each block as in the encryption by the decrypting part 421 so that the influence of the alteration of the encrypted physical characteristic information is exerted only locally on the portion which is obtained by decrypting the altered portion, but not on the other portion.

[0059] As illustrated in Fig. 5, therefore, pseudo fluctuations can be synthesized in the decrypted fingerprint data by fraudulently acquiring the encrypted fingerprint data in the network and by altering a portion (as hatched

in Fig. 5) of the encrypted fingerprint data to input as new authenticating information.

[0060] When a portion of the encrypted fingerprint data derived from the portion other than the observing area is altered, as illustrated in Fig. 5, the fingerprint data obtained by the decrypting part 421 are different at the decryption result of the altered portion from the corresponding portion of the original fingerprint data but are completely equivalent in the observing area to the original fingerprint data.

[0061] In other words, the decryption result obtained from the altered encrypted fingerprint data is equivalent over the observing area to the reference data but does not completely match either the reference data or the registered fingerprint data.

[0062] In this case, the variance, caused in the decryption result by altering the encrypted fingerprint data, from the original fingerprint data is regarded as the fluctuations of the fingerprint data by the recognizing deciding part 447, and the fraudulent attack using the altered encrypted fingerprint data may be allowed.

[0063] Therefore, any simple application of the cryptographic technique of the prior art could not enable the system for the identifying by sending and receiving the physical characteristic information through the network, to improve the security, which is expected by utilizing the physical characteristic information.

[0064] It is desirable to provide an elementary technique capable of restoring original physical characteristic information so as to block attacks against the security system by re-utilizing encrypted information.

[0065] It is desirable to provide an identification system utilizing the authenticating information generated according to the physical characteristic information.

[0066] According to one aspect of the present invention there is provided a cryptographic method comprising the steps of: receiving physical characteristic information representing a characteristic inherent to an individual; randomly determining a numeric key; generating a cryptographic key from said numeric key and a predetermined primary key; encrypting said physical characteristic information using said cryptographic key and; generating an auxiliary code for decrypting said cryptographic key, from the encrypted physical characteristic information and said numeric key.

[0067] In this cryptographic method, the auxiliary code depends upon the encrypted physical characteristic information. Therefore, the cryptographic key to be restored according to the auxiliary code necessarily depends upon the physical characteristic information. So by forming cryptogram from the encrypted physical characteristic information and the auxiliary code, the cryptographic key to be utilized for decrypting the encrypted physical characteristic information depends upon the entire cryptogram.

[0068] According to another aspect of the present invention there is provided a decryption method comprising the steps of: receiving an encrypted physical characteristic information and an auxiliary code; restoring a numeric key from said received data; restoring cryptographic key from said numeric key and a predetermined primary key; and decrypting said encrypted physical characteristic information by using said cryptographic key and obtaining physical characteristic information. using the cryptographic key.

[0069] In this decryption method, the original physical characteristic information can be restored by decrypting the encrypted physical characteristic information obtained by the aforementioned cryptographic method, using the cryptographic key assumed to be used in encrypting physical characteristic information.

[0070] The invention also provides computer programs as described above in any of the storage medium aspects of the invention.

[0071] Preferred features of the present invention will now be described, purely by way of example, with reference to the accompanying drawings, in which:-

Fig. 1 is a diagram showing an example of the construction of a remote identification system of the prior art;

Fig. 2 is a diagram showing an example of the construction of the identification system of the prior art, utilizing the physical characteristic information;

Fig. 3 is a diagram for explaining the comparing processing on physical characteristics;

Fig. 4 is a diagram showing an example of the construction of the remote identification system utilizing the physical characteristic information; and

Fig. 5 is a diagram for explaining effects from alterations of the physical characteristic information.

Fig. 6 is a diagram illustrating the principles of a cryptographic method and a decrypting method according to one of the preferred embodiments of the invention;

Fig. 7 is a block diagram illustrating the principles of a cryptographic equipment anda decrypting equipment according to one of the preferred embodiments of the invention;

Fig. 8 is a diagram showing an embodiment of the invention;

Fig. 9 is a flow chart showing the operations of the embodiment of Fig. 8;

Fig. 10 is a diagram for explaining the operations of the embodiment of Fig. 8;

[0072] First of all, here will be described the principles of a cryptographic method and a decrypting method, a cryptographic equipment and a decrypting equipment, and an identification system according to a preferred embodiment of the invention. Fig. 6A is a diagramillustrating the principle of a cryptographic method according to one of the preferred embodiments of the invention.

[0073] The cryptographic method, as shown in Fig. 6A, is constructed to include: a step (S11) of inputting physical characteristic information; a step (S12) of determin-

ing a numeric key; a step (S13) of generating a cryptographic key; an encryption step (S14) ; and a step (S15) of generating an auxiliary code.

[0074] The principle of the cryptographic method according to one of the preferred embodiments of the invention will be described in the following.

[0075] In the inputting step (S11), the physical characteristic information representing a characteristic inherent to an individual is received. In the numeric key determining step (S12), a numeric key is determined randomly. In the cryptographic key generating step (S13), the cryptographic key is generated from the numeric key and a predetermined primary key. In the encryption step (S14), the physical characteristic information is encrypted by using the cryptographic key. In the code generating step (S15), an auxiliary code is generated from the encrypted physical characteristic information and the numeric key.

[0076] The operations of the cryptographic method will be described in the following.

[0077] At each encryption, according to the numeric key determined at the numeric key determining step (S12), the cryptographic key is generated at the cryptographic key generating step (S13), and the physical characteristic information inputted at the inputting step (S11) is encrypted at the encryption step (S14) by using that cryptographic key. According to the encrypted physical characteristic information thus obtained and the aforementioned numeric key, on the other hand, the auxiliary code is generated at the code generating step (S15).

[0078] Thus, a depending relationship is established between the auxiliary code and the encrypted physical characteristic information.

[0079] By providing the encrypted physical characteristic information and the auxiliary code for the decryption and by restoring the cryptographic key in the decryption according to the aforementioned auxiliary code, therefore, the decryption of the encrypted physical characteristic information is carried out by the cryptographic key depending up on the encrypted physical characteristic information.

[0080] Fig. 6B is a diagram illustrating the principle of the decrypting method according to one of the preferred embodiments of the invention.

[0081] The decrypting method, as shown in Fig. 6B, include a receiving step (S21), a numeric key restoring step (S22), a cryptographic key restoring step (S23) and a decrypting step (S24).

[0082] The principle of the decrypting method according to one of the preferred embodiments of the invention will be described in the following.

[0083] In the receiving step (S21), an encrypted physical characteristic information and an auxiliary code are received as a cryptogram. In the numeric key restoring step (S22), a numeric key is restored from the encrypted physical characteristic information and the auxiliary code. Next, in the cryptographic key restoring step (S23), a cryptographic key is restored from the numeric key and a predetermined primary key. In the decrypting step (S24), the encrypted physical characteristic information is decrypted by using the cryptographic key and physical characteristic information is restored.

[0084] The operations of the decrypting method will be described in the following.

[0085] When the receiving step (S21) receives the encrypted physical characteristic information and the auxiliary code, the numeric key is restored at the numeric key restoring step (S22), and the cryptographic key is restored at the cryptographic key restoring step (S23) according to the numeric key and the primary key. It depends upon the propriety of the encrypted physical characteristic information whether or not the cryptographic key thus obtained is correct. Only when the proper encrypted physical characteristic information arrives, therefore, the original physical characteristic information can be restored at the restoring step (S24).

[0086] Fig. 7A is a block diagram showing the principle of a cryptographic equipment according to one of the preferred embodiments of the invention.

[0087] The cryptographic equipment, as shown in Fig. 7A, is constructed to include physical characteristic inputting section 111, numeric key determining section 112, keygenerating section 113, encrypting section 114, generating section 115 and combining section 116.

[0088] The principle of the cryptographic equipment according to one of the preferred embodiments of the invention will be described in the following.

[0089] The physical characteristic inputting section 111 inputs physical characteristic information representing a characteristic inherent to an individual. The numeric key determining section 112 determines a numeric key randomly. The key generating section 113 generates a cryptographic key from the numeric key and a predetermined primary key. The encrypting section 114 encrypts the inputted physical characteristic information by using the cryptographic key. The code generating section 115 generates an auxiliary code from the encrypted physical characteristic information and the numeric key.

[0090] The operations of the cryptographic equipment thus constructed will be described in the following.

[0091] At each encryption, the numeric key is generated by the numeric key determining section 112, and this numeric key is used to generate the cryptographic key by the key generating section 113. When the encrypting section 114 performs the encryption by using the cryptographic key, therefore, the physical characteristic information inputted by the inputting section 111, is encrypted by using a onetime cryptographic key. According to the encrypted physical characteristic information thus obtained and the aforementioned numeric key, on the other hand, the auxiliary code is generated by the code generating section 115.

[0092] Thus, the auxiliary code is generated according to the encrypted physical characteristic information so that a depending relationship is established between the auxiliary code and the encrypted physical characteristic information.

[0093] So, a cryptogram generated from the encrypted physical characteristic information and auxiliary code is subjected to decrypting processing, the cryptographic key in the decryption is restored according to the aforementioned auxiliary code. Therefore, the decryption of the encrypted physical characteristic information is performed by the cryptographic key depending upon the encrypted physical characteristic information.

[0094] Fig. 7B is a block diagram illustrating the principle of a decrypting equipment according to one of the preferred embodiments of the invention.

[0095] The decrypting equipment, as shown in Fig. 7B, is constructed to include receiving section 117, numeric key restoring section 118, the key generating section 113 and decrypting section 119.

[0096] The principle of the decrypting equipment according to one of the preferred embodiments of the invention will be described in the following.

[0097] The receiving section 117 receives the encrypted physical characteristic information and an auxiliary code. The numeric key restoring section 118 restores a numerickey from the encrypted physical characteristic information and the auxiliary code. The key generating section 113 generates a cryptographic key from the numeric key and a predetermined primary key. The decrypting section 119 decrypts the encrypted physical characteristic information by using the cryptographic key.

[0098] The operations of the decrypting equipment thus constructed will be described in the following.

[0099] According to the encrypted physical characteristic information and the auxiliary code received through the receiving section 117, the numeric key is restored by the numeric key restoring section 118, and the cryptographic key is generated by the key generating section 113 according to the restored numeric key.

[0100] It depends upon the propriety of the encrypted physical characteristic information whether or not the cryptographic key thus obtained is correct. Only when the proper encrypted physical characteristic information arrives, therefore, the original physical characteristic information can be restored by the decrypting section 119.

[0101] On the other hand, a encryption program according to one of the preferred embodiments of the invention is constructed to include an inputting procedure, a numeric key determining procedure, a cryptographic key generating procedure, an encrypting procedure and a code generating procedure.

[0102] The principle of the encryption program according to one of the preferred embodiments of the invention will be described in the following.

[0103] In the inputting procedure, physical characteristic information representing a characteristic inherent to an individual is inputted. In the numeric key determining procedure, a numeric key is randomly determined. In the key generating procedure, a cryptographic key is generated from the numeric key and a predetermined primary key. In the encrypting procedure, the inputted physical characteristic information is encrypted by using the cryptographic key. In the code generating procedure, an auxiliary code is generated according to the encrypted physical characteristic information and the numeric key.

[0104] The operations of the encryption program thus constructed will be described in the following.

[0105] The numeric key obtained by the numeric key determining procedure is used to generate the onetime cryptographic key by the keygenerating procedure, and the physical characteristic information inputted in the inputting procedure is encrypted in the encrypting procedure by the aforementioned cryptographic key. In the code generating procedure, on the other hand, the auxiliary code is generated according to the encrypted physical characteristic information and the aforementioned numeric key.

[0106] Thus, a depending relationship is established between the auxiliary code and the encrypted physical characteristic information. The restoration of the original physical characteristic information is assured, so long as the encrypted physical characteristic information and the auxiliary code are subjected as they are to the decrypting processing, but is completely impossible according to the alteration of the encrypted physical characteristic information or the auxiliary code.

[0107] On the other hand, a decryption program according to one of the preferred embodiments of the invention is constructed to include a receiving procedure, a numeric key restoring procedure, a key generating procedure and a decrypting procedure. The principle of the decryption program according to one of the preferred embodiments of the invention will be described in the following.

[0108] In the receiving procedure, a cryptogram including the encrypted physical characteristic information and an auxiliary code are received. In the numeric key restoring procedure, a numeric key for the generation of a cryptographic key is restored according to the encrypted physical characteristic information and the auxiliary code. In the key generating procedure, a cryptographic key is generated according to the numeric key and a predetermined primary key. In the decrypting procedure, the encrypted physical characteristic information is decrypted by using the cryptographic key.

[0109] The operations of the decryption program thus constructed will be described in the following.

[0110] According to the encrypted physical characteristic information and the auxiliary code received in the receiving procedure, the numeric key is restored by the numeric key restoring procedure, and the cryptographic key is generated by the key generating procedure according to the numeric key.

[0111] By utilizing a depending relationship between the encryptedphysical characteristic information and the auxiliary code, therefore, the cryptographic key used in the encryption can be restored and subjected to the decrypting procedure only when both the encrypted physical characteristic information and the auxiliary code are correct.

[0112] An embodiment of the invention will be described in detail with reference to the accompanying drawings.

[0113] Fig. 8 shows an embodiment of the present invention, and Fig. 9 is a flow chart showing the encryption and the decryption.

[0114] In Fig. 8, the components having the same functions and constructions as those shown in Figs. 2 and 4 are designated by the common reference numerals, and their description will be omitted.

[0115] In a client-side identification equipment 201 shown in Fig. 8, the fingerprint data obtained by the fingerprint reader 430 (see Fig. 2) are encrypted by a cryptographic equipment 210, and the encrypted physical characteristic information obtained is sent by the transmission controlling part 413 to the network.

[0116] In a server-side identification equipment 202, on the other hand, the encrypted physical characteristic information received by the transmission controlling part 422 is decrypted by a decrypting equipment 220 so that the result of this decryption is subjected to the processing of the fingerprint identification equipment 440.

[0117] In the cryptographic equipment 210 shown in Fig. 8, a bit pattern generating part 211 generates a cyclic code for cyclic redundancy check (CRC) of a predetermined length according to a series of numeric data representing the fingerprint data inputted (at Steps 301 and 302 in Fig. 9A), and the generated cyclic code is subjected as the numeric key to the processing of a key generating part 212.

[0118] Here, the fingerprint data obtained by the aforementioned fingerprint reader 430 contain not only information representing characteristics inherent to the person to be measured (hereunder referred to as "inherent characteristics") and also fluctuation elements fluctuating with the condition of measurement. If a cyclic code of n-bits is generated by the aforementioned bit pattern generating part 211 according to a bit string representing the fluctuation elements, therefore, a bit pattern different for each input of fingerprint data never fails to be obtained but can be utilized as a numeric key changing at each encryption.

[0119] In other words, the bit pattern generating part 211 thus operates to transfer the bit pattern as numeric key obtained to the key generating part 212 so that random numeric data can be generated as a cryptographic key by utilizing the fluctuation of the fingerprint data.

[0120] In Fig. 8, on the other hand, a primary key storage area 213 stores a bit string of a length of n-bits as the primary key, and the key generating part 212 performs an exclusive OR operation between the primary key and the aforementioned bit pattern, for example, to generate a cryptographic key of n-bits (at Step 303 of Fig. 9A) and to subj ect the generated cryptographic key to the processing of a block encrypting part 214.

[0121] When a device password is registered in advance as information for identifying the client-side identification equipment 201, for example, the device password or its portion may be stored as the primary key in the primary key storage area 213. On the other hand, a user's password inputted by the person can be utilized as the primary key. Moreover, a bit pattern obtained by combining the device password and the user's password may be stored as the primary key in the primary key storage area 213.

[0122] In general, the longer the cryptographic key is, the more difficult the decryption of the encrypted information becomes, so that a bit pattern of 32 bits or longer should be generated as the cryptographic key.

[0123] In particular, a cyclic code of 56 bits is generated by the bit pattern generating part 211, and a bit pattern of the same length is stored as the primary key. If the cryptographic key of 56 bits is then generated by the key generating part 212, the block encryption such as the data encryption standard method can be applied.

[0124] In this case, the block encrypting part 214 may be constructed to encrypt the fingerprint data by using the aforementioned cryptographic key in accordance with the data encryption standard method (at Step 304 of Fig. 9A) and to subj ect the obtained encrypted fingerprint data to the processings of a hash coding part 215 and of a message combining part 216. This hash coding part 215 is constructed to convert the encrypted fingerprint data, for example, into a hash address represented as a bit string shorter than their own length by using a proper hash function.

[0125] The hash address obtained by the hash coding part 215 is inputted together with the aforementioned numeric key to a logical operating part 217. This logical operating part 217 performs a predetermined logic operation to convert a combination of the hash address and the numeric key by a one-to-one mapping function and to transfer the result of operation to the message combining part 216.

[0126] Here, if a hash function having a sufficient diffusion is used in the aforementioned hash coding part 215, this hash coding part 215 can operate in response to an input of the encrypted data on the fingerprint characteristics to obtain a digest reflecting the summary of the encrypted fingerprint characteristic data (at Step 305 of Fig. 9A).

[0127] In response to the input of the hash address and the numeric key, on the other hand, the logical operatingpart 217 calculates their exclusive OR (at Step 306 of Fig. 9A) so that the two inputs can be converted into a mapping corresponding one-to-one to their combination thereby to obtain the result of logic operation reflecting both the hash address and the numeric key.

[0128] In this case, the aforementioned hash coding part 215 and logical operating part 217 can perform a simple arithmetic and logical operation to obtain an auxiliary code reflecting both a digest related closely to encrypted fingerprint characteristic data and the numeric key.

[0129] By thus generating a depending relationship between the auxiliary code and the encrypted fingerprint

characteristic data, the cryptographic key to be utilized in the decrypting equipment changes depending upon both the auxiliary code and the encrypted fingerprint characteristic data, as will be described later, so that the restoration of the cryptographic key can be made impossible in response to the alteration of a cryptogram to be transmitted through the network.

[0130] On the other hand, the message combining part 216 shown in Fig. 8 combines the encrypted fingerprint characteristic data received from the block encrypting part 214 and the aforementioned auxiliary code (at Step 307 of Fig. 9A), for example, to generate the authenticatinginformation represented as a series of bit string, as illustrated in Fig. 10, and to send the authenticating information to the network by the transmission controlling part 413.

[0131] Thus, in response to the inputs of the encrypted fingerprint characteristic data and the auxiliary code, the message combining part 216 can operate to combine the encrypted fingerprint characteristic data and the auxiliary code and to send them to the network by the transmission controlling part 413.

[0132] Next, a decrypting equipment of the first embodiment will be described in detail.

[0133] In the decrypting equipment 220 shown in Fig. 8, an auxiliary code separating part 222 receives the authenticating information shown in Fig. 10 from the transmission controlling part 422 (at Step 311 of Fig.9B), and separates the authenticating information into the encrypted fingerprint characteristic data (at Step 312 of Fig. 9B) and the auxiliary code to send the encrypted fingerprint characteristic data to a block decrypting part 223 and a hash coding part 224 and to send the auxiliary code to a logical operating part 225.

[0134] Here, the auxiliary code is the result of exclusive OR operation of the hash address corresponding to the encrypted fingerprint characteristic data and the numeric key, as has been described above.

[0135] Therefore, the hash address of the encrypted fingerprint characteristic data is determined by the hash coding part 224 by using the same hash function as that used in the encryption (at Step 313 of Fig. 9B), and the exclusive OR between the hash address and the auxiliary code is determined by the logical operating part 225 (at Step 314 of Fig. 9B), so that the numeric key used for generating the cryptographic key can be restored.

[0136] In Fig. 8, on the other hand, a primary key storage area 226 stores the primary key used in the encryption, and the primary key storage area 226 and a key generating part 227 can operate, in response to the result of operation by the logical operating part 225 as the numeric key, to reproduce the cryptographic key used in the encryption and to subject the reproduced cryptographic key to the processing of the block decrypting part 223(at Steps 315 and 316 of Fig. 9B).

[0137] Thus, the decrypting equipment can be realized to restore the original fingerprint data from the authenticating information containing the encrypted fingerprint characteristic data obtained by the aforementioned cryptographic equipment 210.

[0138] Next, here will be described a method for blocking a fraudulent access by the server-side identification equipment 202 including the fingerprint identification equipment 440 of the aforementioned construction when the authenticating information is partially altered in the course of being transmitted in the network.

[0139] If the encrypted fingerprint characteristic data contained in the authenticating information is partially altered (as hatched in Fig. 10), as shown in Figs. 10A and 10B, the hash address obtained by the hash coding part 224 is naturally different according to the input of the encrypted fingerprint characteristic data from that which is obtained by hash-coding the original encrypted fingerprint characteristic data.

[0140] In this case, an erroneous digest is obtained by the alteration of the encrypted fingerprint characteristic data so that the numeric key obtained by inputting the erroneous digest and the auxiliary code to the logical operating part is also erroneous. Naturally, the error is also propagated to the cryptographic key that is restored by the key generating part 227 according to that numeric key.

[0141] As a result, the block decrypting part 223 decrypts the altered encrypted fingerprint characteristic data by using the erroneous cryptographic key so that the result of decryption can be expected to be remarkably different from the original fingerprint data.

[0142] When the auxiliary code included in the authenticating information is altered, as shown in Fig. 10B, the correct hash address can be obtained by the hash coding part 224 in response to the input of the encrypted fingerprint characteristic data. However, since the auxiliary code is erroneous, the result of operation by the logical operating part will be erroneous, making the resulting numeric key different from the original numeric key.

[0143] In this case, too, the erroneous cryptographic key is subjected to the processing of the block decrypting part 223 as in the case where the encrypted fingerprint data are altered, so that the result of decryption obtained by the block decrypting part 223 can also be expected to be remarkably different from the original fingerprint data.

[0144] From this, altering the authenticating information even partially results in the breaking of the depending relationship formed in the encryption between the encrypted physical characteristic information and the auxiliary code, and the influence of this alteration can be propagated to the entire result of decryption.

[0145] Since the difference between the result of decryption obtained by using the erroneous cryptographic key and the original fingerprint data is serious as described above, it canbe reliably decided by the fingerprint identification equipment 440 that the fingerprint data obtained in response to the input of the altered authenticating information do not belong to the eligible person.

[0146] This is because the influence of the alteration

of an arbitrary portion of the authenticating information is exerted all over the result of decryption. It can therefore be expected that the information comprising to the observing area in the fingerprint identification equipment 440 is reliably influenced considerable amount.

[0147] Irrespective of the extent of the observing area, therefore, the fingerprint data restored from the altered authenticating information are reliably decided as not provided in the eligible person by the dactyloscopy. This makes it possible to reliably block the access according to the encrypted physical characteristic information fraudulently acquired.

[0148] Constructing to exclude the fingerprint data, which are identical to the reference data or the registered fingerprint data, when inputted, as the "replay attack" is adopted as in the fingerprint identification equipment 440 shown in Fig. 4, it is possible to block the access utilizing the fraudulently acquired authenticating information as it is.

[0149] In the first embodiment, the features of the inherent characteristics and the fluctuation elements included in the physical characteristic information are individually utilized to identify a person reliably to provide a remote identification system of high safety.

[0150] Here, the cryptographic method to be adopted in the encrypting part 214 may be one of the common key system, and an affine transformation cryptography or a vegenere cryptography may be adopted in place of the aforementioned data encryption standard method.

[0151] On the other hand, the unit length of encryption by the encrypting part 214 can also be modified.

[0152] In this modification, for example, the encryption unit has a length of 32 bits, and both the primary key and the numeric key are given 32 bits. The key generating part 212 generates a cryptographic key of 32 bits, and the encrypting part 214 determines random numbers sequentially for each block by utilizing that cryptographic key so that the series of result of exclusive OR operation between each random number and the corresponding block may be used as the result of encryption.

[0153] On the other hand, the digest of the encrypted physical characteristic information may depend upon the encrypted physical characteristic information as a whole. For example, therefore, the cryptographic equipment and the decrypting equipment may be constructed to include a decimating part for decimating bits simply from the bit string representing the encrypted physical characteristic information, to generate the digest, in place of the hash coding parts 215 and 224. Alternatively, the cryptographic equipment and the decrypting equipment can also be constructed to include a cyclic code generating part for generating the cyclic code on the encrypted physical characteristic information as the digest.

[0154] On the other hand, the client-side identification equipment 201 may be constructed to include an integrated circuit card writer in place of the transmission controlling part 413 shown in Fig. 8, and the server-side identification equipment 202 may be constructed to include an integrated circuit card reader in place of the transmission controlling part 422, so that the authenticating information may be sent and received by using the integrated circuit card.

[0155] In this case, the authenticating information can be transferred to the server-side identification equipment 202 by manually transporting the nameplate having the integrated circuit card (hereunder referred to as "IC card").

[0156] On the other hand, the program to be executed by the comput er can realize the functions of the individual parts constructing the decrypting equipment 220 shown in Fig. 8. By recording the program in the storage media and distributing it, the system for encrypting the physical characteristic information safely by using the cryptographic method can be provided for users of wide range.

[0157] Likewise, the program for executing the computer can realize the functions of the individual parts constructing the decrypting equipment 220 shown in Fig. 8. By recording the program in the storage media and distributing it, there can be provided the system for decrypting only the proper authenticating information encrypted by using the first cryptographic method, correctly to restore the physical characteristic information and to subject it to the identifying processing.

Claims

1. A cryptographic method comprising the steps of:

   receiving physical characteristic information representing a characteristic inherent to an individual (S11);
   randomly determining a numeric key (S12);
   generating a cryptographic key from said numeric key and a predetermined primary key (S13);
   encrypting said physical characteristic information using said cryptographic key (S14); and
   generating an auxiliary code for restoring said cryptographic key, from said encrypted physical characteristic information and said numeric key (S15).

2. A decryption method comprising the steps of:

   receiving encrypted physical characteristic information and an auxiliary code (S21);
   restoring a numeric key from said received data (S22);
   restoring cryptographic key from said numeric key and a predetermined primary key (S23); and
   decrypting said encrypted physical characteristic information by using said cryptographic key and obtaining physical characteristic information (S24).

3. A cryptographic equipment, comprising:

inputting means (111) for inputting physical characteristic information representing a characteristic inherent to an individual;
numeric key generating means (112) for randomly determining numeric key;
key generating means (113) for generating a cryptographic key from said numeric key and a predetermined primary key;
encrypting means (114) for encrypting said physical characteristic information using said cryptographic key; and
code generating means (115) for generating an auxiliary code from said encrypted physical characteristic information and said numeric key.

4. A decryption equipment comprising:

receiving means (117) for receiving an encrypted physical characteristic information and an auxiliary code;
numeric key restoring means (118) for restoring a numeric key from said encrypted physical characteristic information and said auxiliary code;
key generating means (113) for generating a cryptographic key from said numeric key and a predetermined primary key; and
decrypting means (119) for decrypting said encrypted physical characteristic information by using said cryptographic key.

5. A computer-readable medium that stores instructions which cause at least a portion of a computer system to perform:

an inputting procedure for inputting physical characteristic information representing a characteristic inherent to an individual
a numeric key generating procedure for randomly determining a numeric key;
a key generating procedure for generating a cryptographic key from said numeric key and a predetermined primary key;
an encrypting procedure for encrypting said physical characteristic information using said cryptographic key; and
a code generating procedure for generating an auxiliary code from said encrypted physical characteristic information and said numeric key.

6. A computer-readable medium that stores instructions which cause at least a portion of a computer system to perform:

a receiving procedure for receiving a cryptogram including an encrypted physical characteristic information and an auxiliary code;
a numeric key restoring procedure for restoring a numeric key from said encrypted physical characteristic information and said auxiliary code;
a key generating procedure for generating a cryptographic key from said numeric key and a predetermined primary key; and
a decrypting procedure for decrypting said encrypted physical characteristic information by using said cryptographic key.

Patentansprüche

1. Kryptographisches Verfahren, mit den Schritten:

Empfangen einer physischen charakteristischen Information, die ein einer Person anhaftendes Charakteristikum repräsentiert (S11);
willkürliches Bestimmen eines numerischen Schlüssels (S12);
Erzeugen eines kryptographischen Schlüssels aus dem numerischen Schlüssel und einem vorbestimmten Primärschlüssel (S13);
Verschlüsseln der physischen charakteristischen Information unter Verwendung des kryptographischen Schlüssels (S14); und
Erzeugen eines Hilfscodes zum Wiederherstellen des kryptographischen Schlüssels aus der verschlüsselten physischen charakteristischen Information und dem numerischen Schlüssel (S15).

2. Entschlüsselungsverfahren, mit den Schritten:

Empfangen einer verschlüsselten physischen charakteristischen Information und eines Hilfscodes (S21);
Wiederherstellen eines numerischen Schlüssels aus den empfangenen Daten (S22);
Wiederherstellen eines kryptographischen Schlüssels aus dem numerischen Schlüssel und einem vorbestimmten Primärschlüssel (S23); und
Entschlüsseln der verschlüsselten physischen charakteristischen Information durch Verwenden des kryptographischen Schlüssels und Erhalten einer physischen charakteristischen Information (S24).

3. Kryptographisches Gerät, mit:

Eingabemittel (111), um eine physische charakteristische Information einzugeben, die ein einer Person anhaftendes Charakteristikum repräsentiert;
numerische Schlüssel erzeugendem Mittel

(112), um einen numerischen Schlüssel willkürlich zu bestimmen;
Schlüssel erzeugendem Mittel (113), um aus dem numerischen Schlüssel und einem vorbestimmten Primärschlüssel einen kryptographischen Schlüssel zu erzeugen;
Verschlüsselungsmittel (114), um die physische charakteristische Information unter Verwendung des kryptographischen Schlüssels zu verschlüsseln; und
Codes erzeugendem Mittel (115), um aus der verschlüsselten physischen charakteristischen Information und dem numerischen Code einen Hilfscode zu erzeugen.

4. Entschlüsselungsgerät, mit:

Empfangsmittel (117), um eine verschlüsselte physische charakteristische Information und einen Hllfscode zu empfangen;
numerische Schlüssel wiederherstellendem Mittel (118), um aus der verschlüsselten physischen charakteristischen Information und dem Hilfscode einen numerischen Schlüssel wiederherzustellen;
Schlüssel erzeugendem Mittel (113), um aus dem numerischen Schlüssel und einem vorbesümmten Primärschlüssel einen kryptographischen Schlüssel zu erzeugen; und
Entschlüsselungsmlttel (119), um unter Verwendung des kryptographischen Schlüssels die verschlüsselte physische charakteristische Information zu entschlüsseln.

5. Computerlesbares Medium, das Anweisungen speichert, welche zumindest einen Teil eines Computersystems veranlassen, auszuführen:

eine Eingabeprozedur, um eine physische charakteristische Information einzugeben, die ein einer Person anhaftendes Charakteristikum repräsentiert;
eine numerische Schlüssel erzeugende Prozedur, um einen numerischen Schlüssel willkürlich zu bestimmen;
eine Schlüssel erzeugende Prozedur, um aus dem numerischen Schlüssel und einem vorbestimmten Primärschlüssel einen kryptographischen Schlüssel zu erzeugen;
eine Verschiüsseiungsprozedur, um die physische charakteristische Information unter Verwendung des kryptographischen Schlüssels zu verschlüsseln; und
eine Codes erzeugende Prozedur, um aus der verschlüsselten physischen charakteristischen Information und dem numerischen Schlüssel einen Hilfscode zu erzeugen.

6. Computerlesbares Medium, das Anweisungen speichert, welche zumindest einen Teil eines Computersystems veranlassen, auszuführen:

eine Empfangsprozedur, um ein Kryptogramm zu empfangen, das eine verschlüsselte physische charakteristische Information und einen Hilfscode enthält;
eine numerische Schlüssel wiederherstellende Prozedur, um aus der verschlüsselten physischen charakteristischen Information und dem Hilfscode einen numerischen Schlüssel wiederherzustellen;
eine Schlüssel erzeugende Prozedur, um aus dem numerischen Schlüssel und einem vorbestimmten Primärschlüssel einen kryptographischen Schlüssel zu erzeugen; und
eine Entschlüsselungsprozedur, um die verschlüsselte physische charakteristische Information durch Verwenden des kryptographischen Schlüssels zu entschlüsseln.

Revendications

1. Procédé cryptographique comprenant les étapes suivantes :

recevoir des informations de caractéristique physique représentant une caractéristique inhérente à un individu (S11) ;
déterminer de façon aléatoire une touche numérique (S12) ;
générer une touche cryptographique à partir de ladite touche numérique et d'une touche primaire prédéterminée (S13) ;
chiffrer lesdites informations de caractéristique physique en utilisant ladite touche cryptographique (S14) ; et
générer un code auxiliaire pour restaurer ladite touche cryptographique à partir desdites informations de caractéristique physique chiffrées et de ladite touche numérique (S15).

2. Procédé de déchiffrage comprenant les étapes suivantes :

recevoir des informations de caractéristique physique chiffrées et un code auxiliaire (S21) ;
restaurer une touche numérique à partir desdites données reçues (S22) ;
restaurer une touche cryptographique à partir de ladite touche numérique et d'une touche primaire prédéterminée (S23) ; et
déchiffrer lesdites informations de caractéristique physique chiffrées en utilisant ladite touche cryptographique, et obtenir des informations de caractéristique physique (S24).

3. Equipement cryptographique, comprenant :

des moyens d'entrée (111) pour entrer des informations de caractéristique physique représentant une caractéristique inhérente à un individu ;
des moyens de génération de touche numérique (112) pour déterminer de façon aléatoire une touche numérique ;
des moyens de génération de touche (113) pour générer une touche cryptographique à partir de ladite touche numérique et d'une touche primaire prédéterminée ;
des moyens de chiffrage (114) pour chiffrer lesdites informations de caractéristique physique en utilisant ladite touche cryptographique ; et
des moyens de génération de code (115) pour générer un code auxiliaire à partir desdites informations de caractéristique physique chiffrées et de ladite touche numérique.

4. Equipement de déchiffrage, comprenant :

des moyens de réception (117) pour recevoir des informations de caractéristique physique chiffrées et un code auxiliaire ;
des moyens de restauration de touche numérique (118) pour restaurer une touche numérique à partir desdites informations de caractéristique physique chiffrées et dudit code auxiliaire ;
des moyens de génération de touche (113) pour générer une touche cryptographique à partir de ladite touche numérique et d'une touche primaire prédéterminée ; et
des moyens de déchiffrage (119) pour déchiffrer lesdites informations de caractéristique physique chiffrées en utilisant ladite touche cryptographique.

5. Support lisible par un ordinateur pour stocker des instructions entraînant au moins une partie d'un système informatique à exécuter :

une procédure d'entrée pour entrer des informations de caractéristique physique représentant une caractéristique inhérente à un individu ;
une procédure de génération de touche numérique pour déterminer de façon aléatoire une touche numérique ;
une procédure de génération de touche pour générer une touche cryptographique à partir de ladite touche numérique et d'une touche primaire prédéterminée ;
une procédure de chiffrage pour chiffrer lesdites informations de caractéristique physique en utilisant ladite touche cryptographique ; et
une procédure de génération de code pour générer un code auxiliaire à partir desdites informations de caractéristique physique chiffrées et de ladite touche numérique.

6. Support lisible par un ordinateur pour stocker des instructions entraînant au moins une partie d'un système informatique à exécuter :

une procédure de réception pour recevoir des informations de caractéristique physique chiffrées et un code auxiliaire ;
une procédure de restauration de touche numérique pour restaurer une touche numérique à partir desdites informations de caractéristique physique chiffrées et dudit code auxiliaire ;
une procédure de génération de touche pour générer une touche cryptographique à partir de ladite touche numérique et d'une touche primaire prédéterminée ; et
une procédure de déchiffrage pour déchiffrer lesdites informations de caractéristique physique chiffrées en utilisant ladite touche cryptographique.

Fig. 1 PRIOR ART

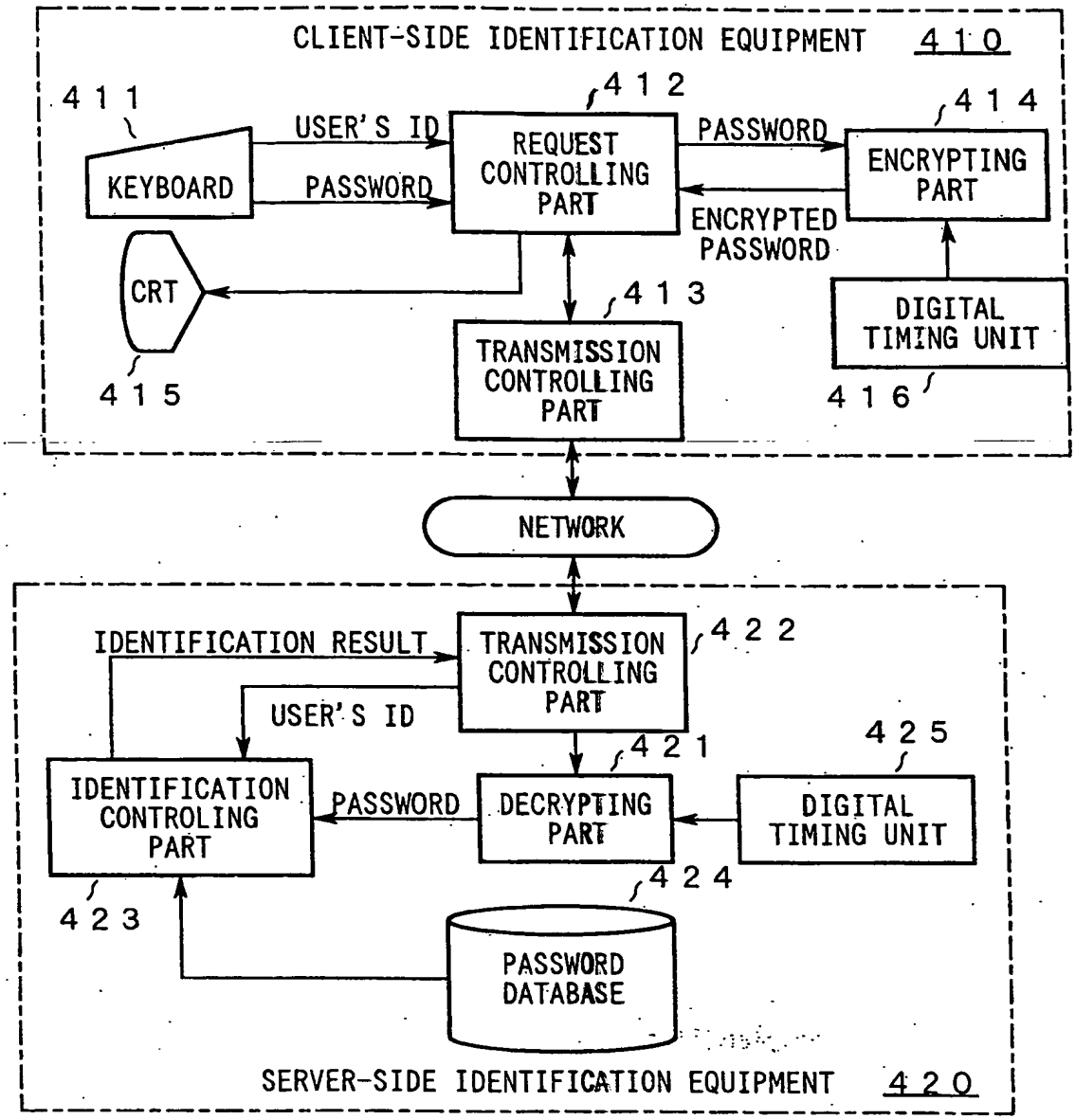


Fig. 2 PRIOR ART

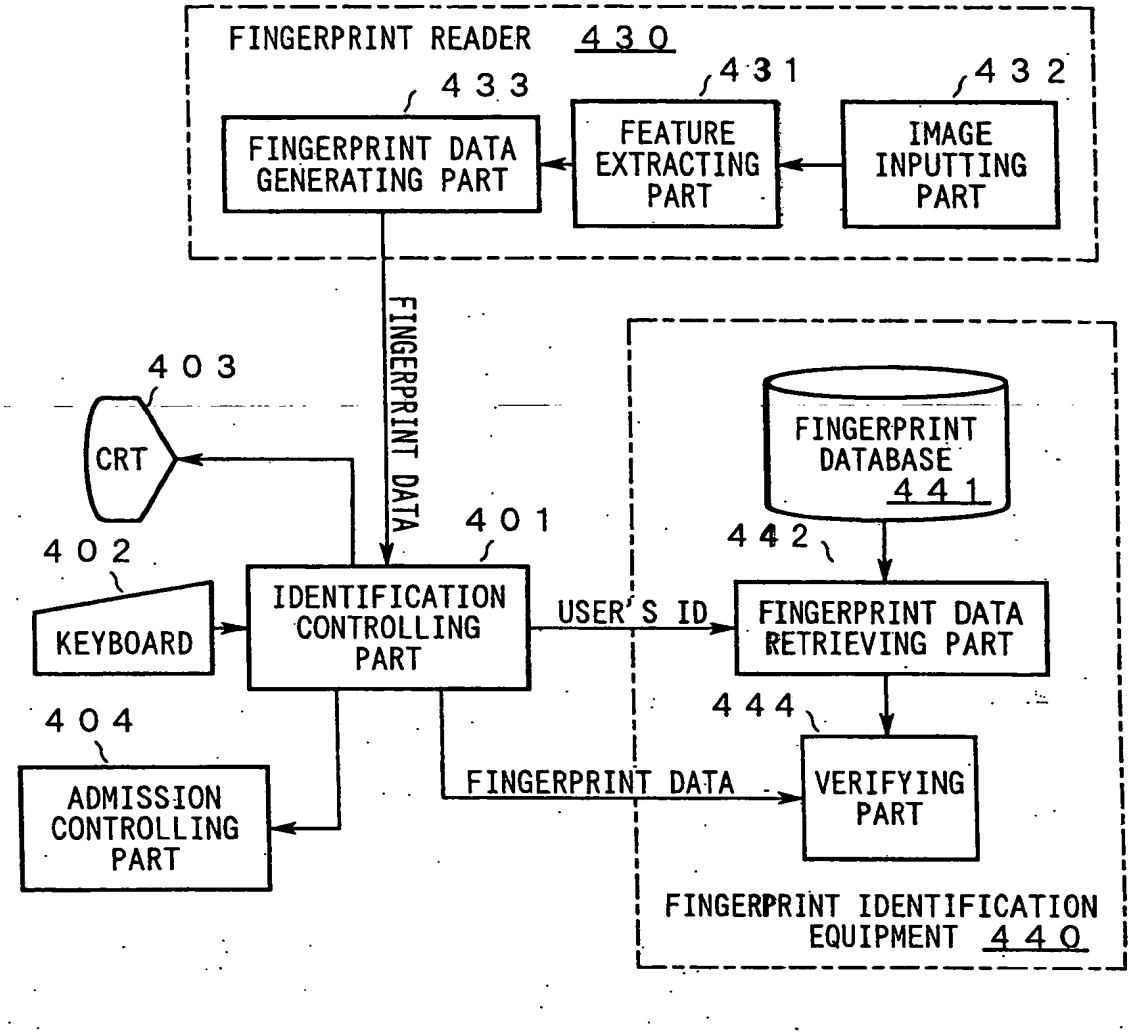


Fig. 3

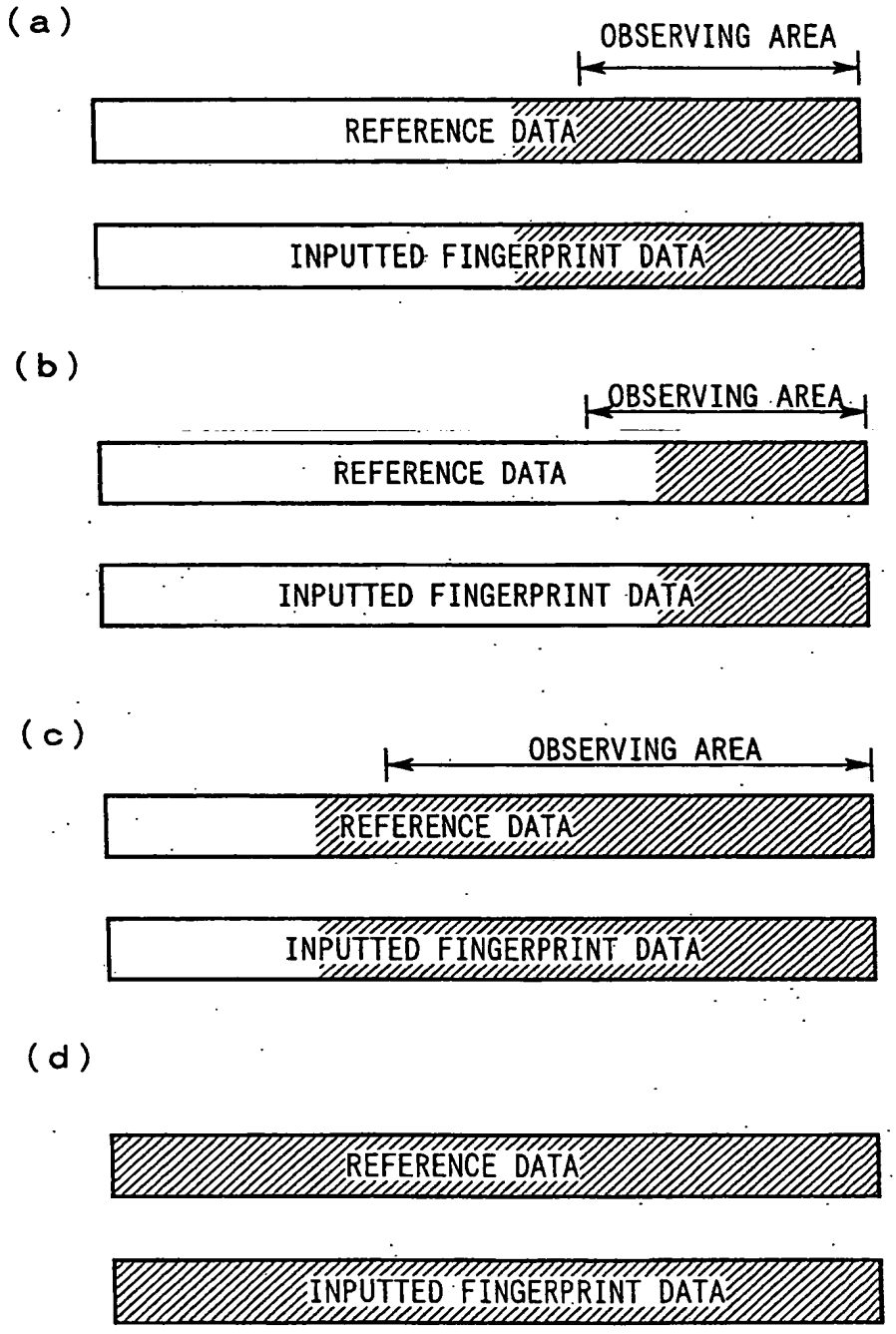

(a)
OBSERVING AREA
REFERENCE DATA
INPUTTED FINGERPRINT DATA
(b)
OBSERVING AREA
REFERENCE DATA
INPUTTED FINGERPRINT DATA
(c)
OBSERVING AREA
REFERENCE DATA
INPUTTED FINGERPRINT DATA
(d)
REFERENCE DATA
INPUTTED FINGERPRINT DATA

Fig. 4

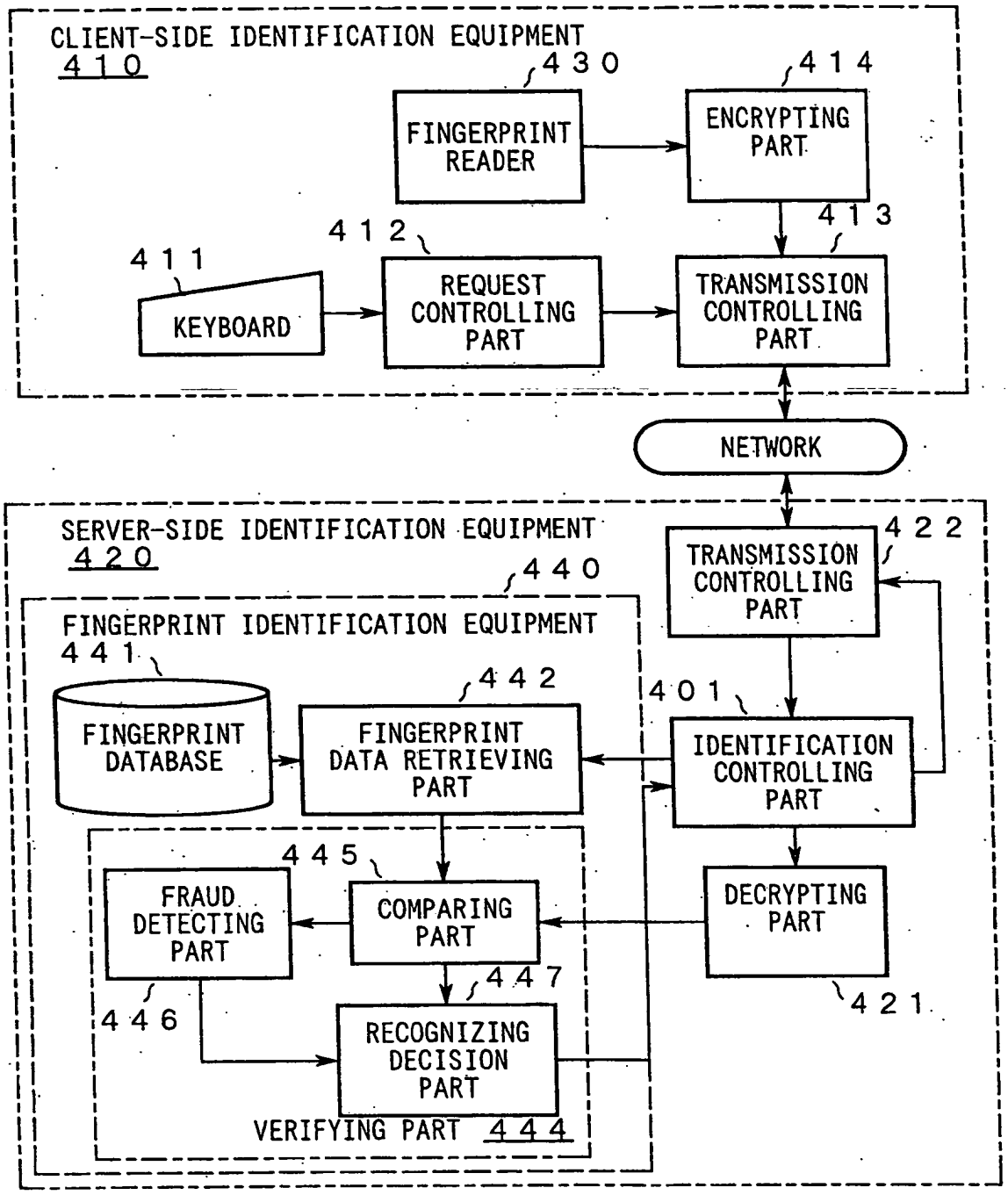

CLIENT-SIDE IDENTIFICATION EQUIPMENT
410
430
FINGERPRINT READER
414
ENCRYPTING PART
413
412
411
KEYBOARD
REQUEST CONTROLLING PART
TRANSMISSION CONTROLLING PART
NETWORK
SERVER-SIDE IDENTIFICATION EQUIPMENT
420
422
TRANSMISSION CONTROLLING PART
440
FINGERPRINT IDENTIFICATION EQUIPMENT
441
442
401
FINGERPRINT DATABASE
FINGERPRINT DATA RETRIEVING PART
IDENTIFICATION CONTROLLING PART
445
FRAUD DETECTING PART
COMPARING PART
DECRYPTING PART
447
446
421
RECOGNIZING DECISION PART
VERIFYING PART 444

Fig. 5

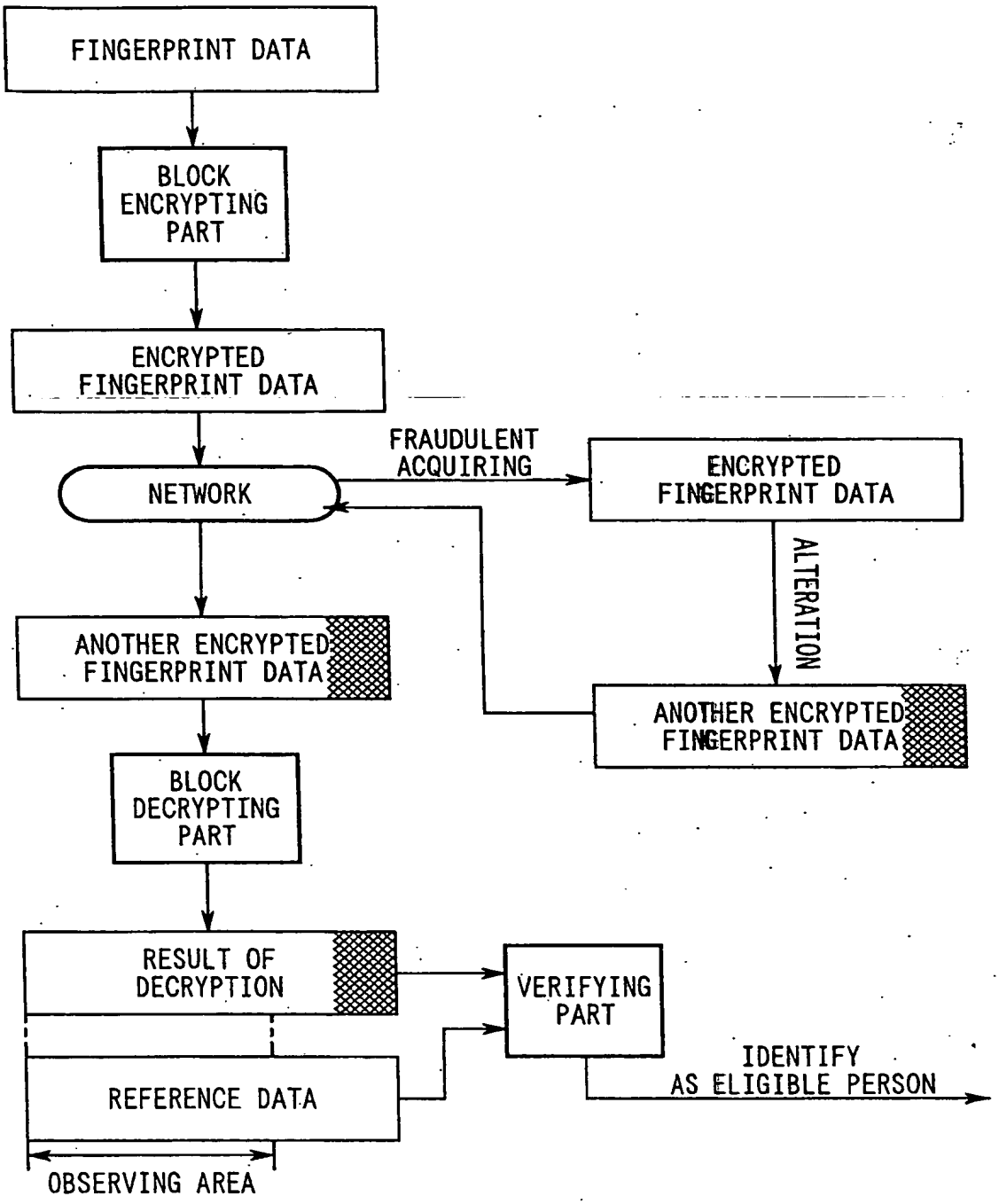

FINGERPRINT DATA
BLOCK ENCRYPTING PART
ENCRYPTED FINGERPRINT DATA
NETWORK
FRAUDULENT ACQUIRING
ENCRYPTED FINGERPRINT DATA
ALTERATION
ANOTHER ENCRYPTED FINGERPRINT DATA
ANOTHER ENCRYPTED FINGERPRINT DATA
BLOCK DECRYPTING PART
RESULT OF DECRYPTION
VERIFYING PART
IDENTIFY AS ELIGIBLE PERSON
REFERENCE DATA
OBSERVING AREA

Fig. 6

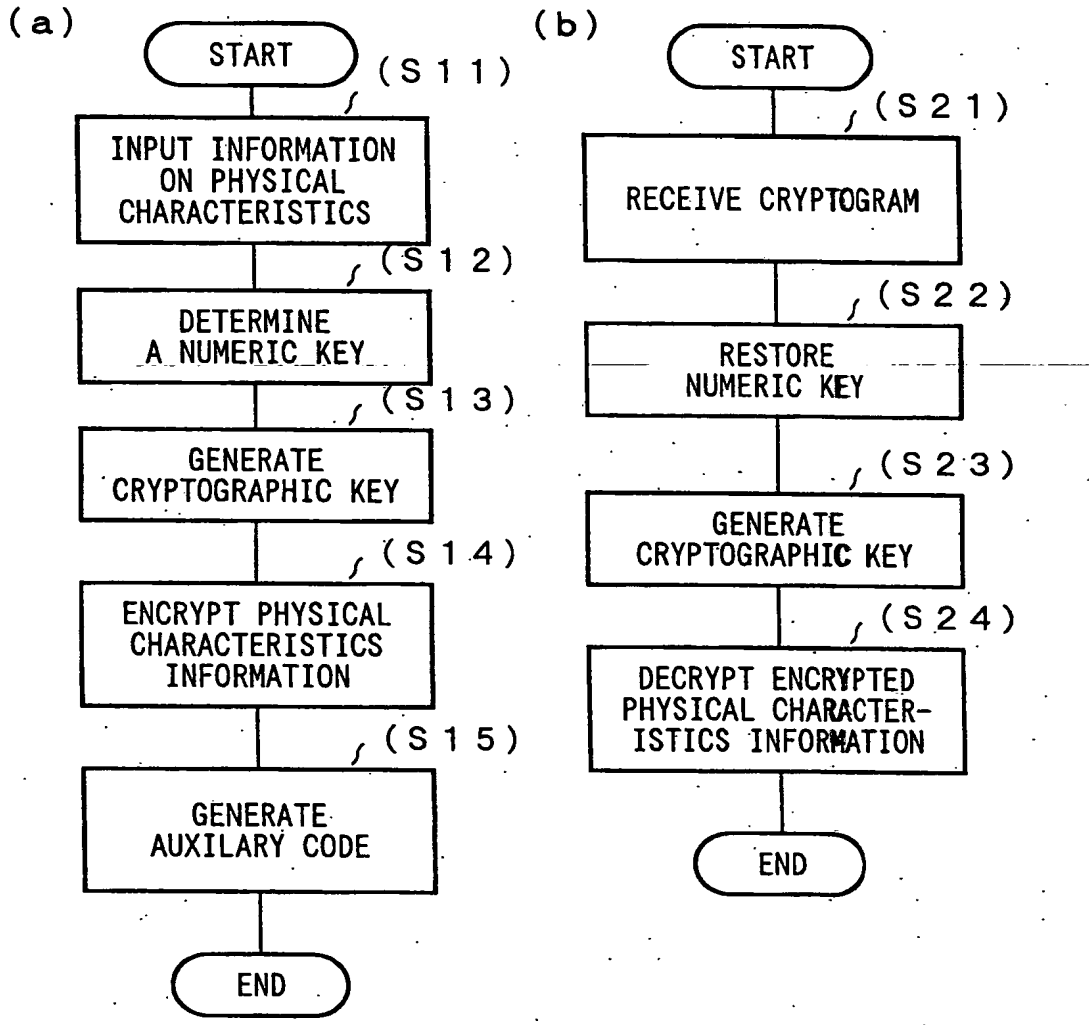

(a)
START
(S11)
INPUT INFORMATION ON PHYSICAL CHARACTERISTICS
(S12)
DETERMINE A NUMERIC KEY
(S13)
GENERATE CRYPTOGRAPHIC KEY
(S14)
ENCRYPT PHYSICAL CHARACTERISTICS INFORMATION
(S15)
GENERATE AUXILARY CODE
END
(b)
START
(S21)
RECEIVE CRYPTOGRAM
(S22)
RESTORE NUMERIC KEY
(S23)
GENERATE CRYPTOGRAPHIC KEY
(S24)
DECRYPT ENCRYPTED PHYSICAL CHARACTER-ISTICS INFORMATION
END

Fig. 7

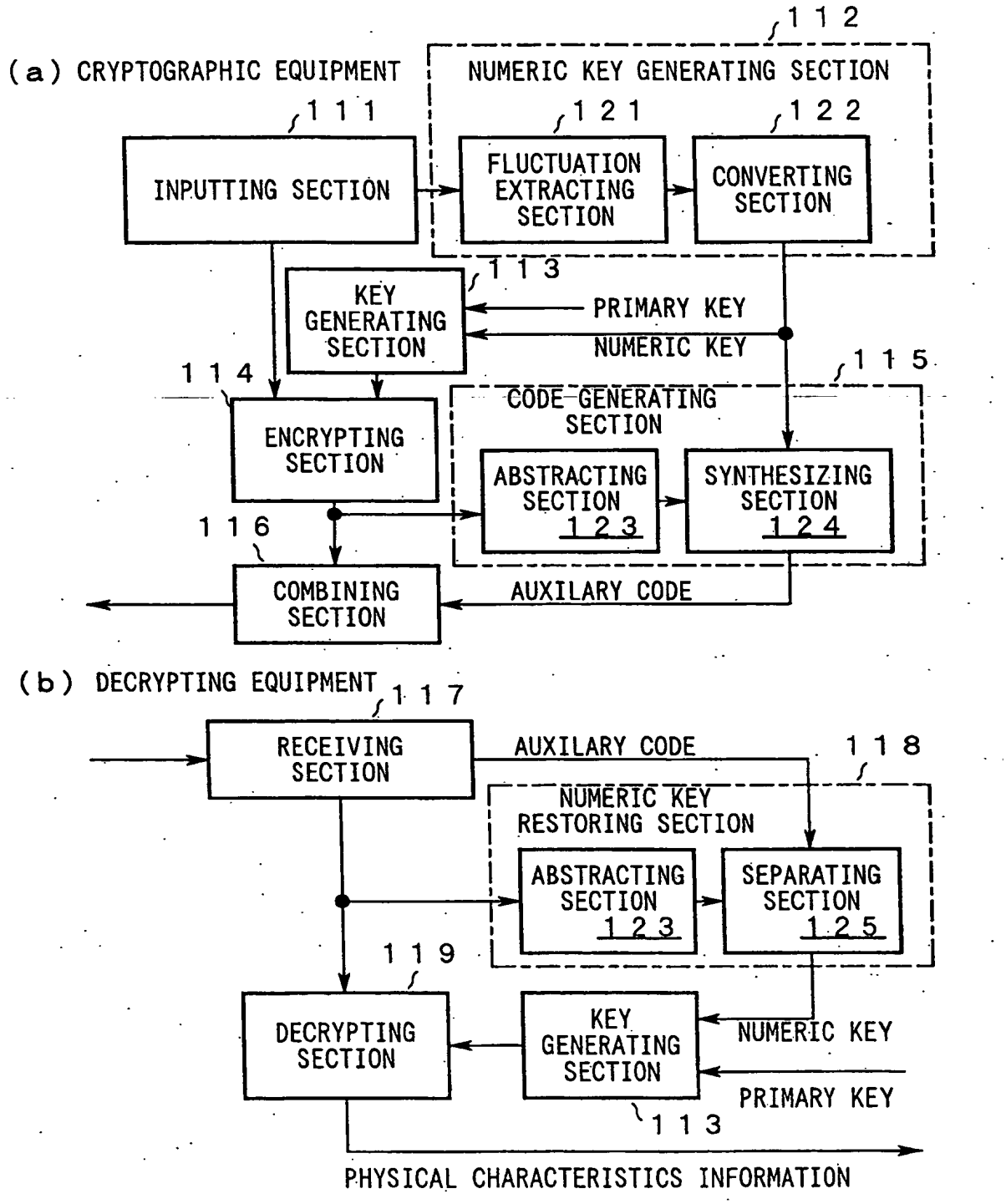

(a) CRYPTOGRAPHIC EQUIPMENT
112
NUMERIC KEY GENERATING SECTION
111
INPUTTING SECTION
121
FLUCTUATION EXTRACTING SECTION
122
CONVERTING SECTION
113
KEY GENERATING SECTION
PRIMARY KEY
NUMERIC KEY
114
ENCRYPTING SECTION
115
CODE GENERATING SECTION
ABSTRACTING SECTION 123
SYNTHESIZING SECTION 124
116
COMBINING SECTION
AUXILARY CODE
(b) DECRYPTING EQUIPMENT
117
RECEIVING SECTION
AUXILARY CODE
118
NUMERIC KEY RESTORING SECTION
ABSTRACTING SECTION 123
SEPARATING SECTION 125
119
DECRYPTING SECTION
KEY GENERATING SECTION
NUMERIC KEY
PRIMARY KEY
113
PHYSICAL CHARACTERISTICS INFORMATION

Fig. 8

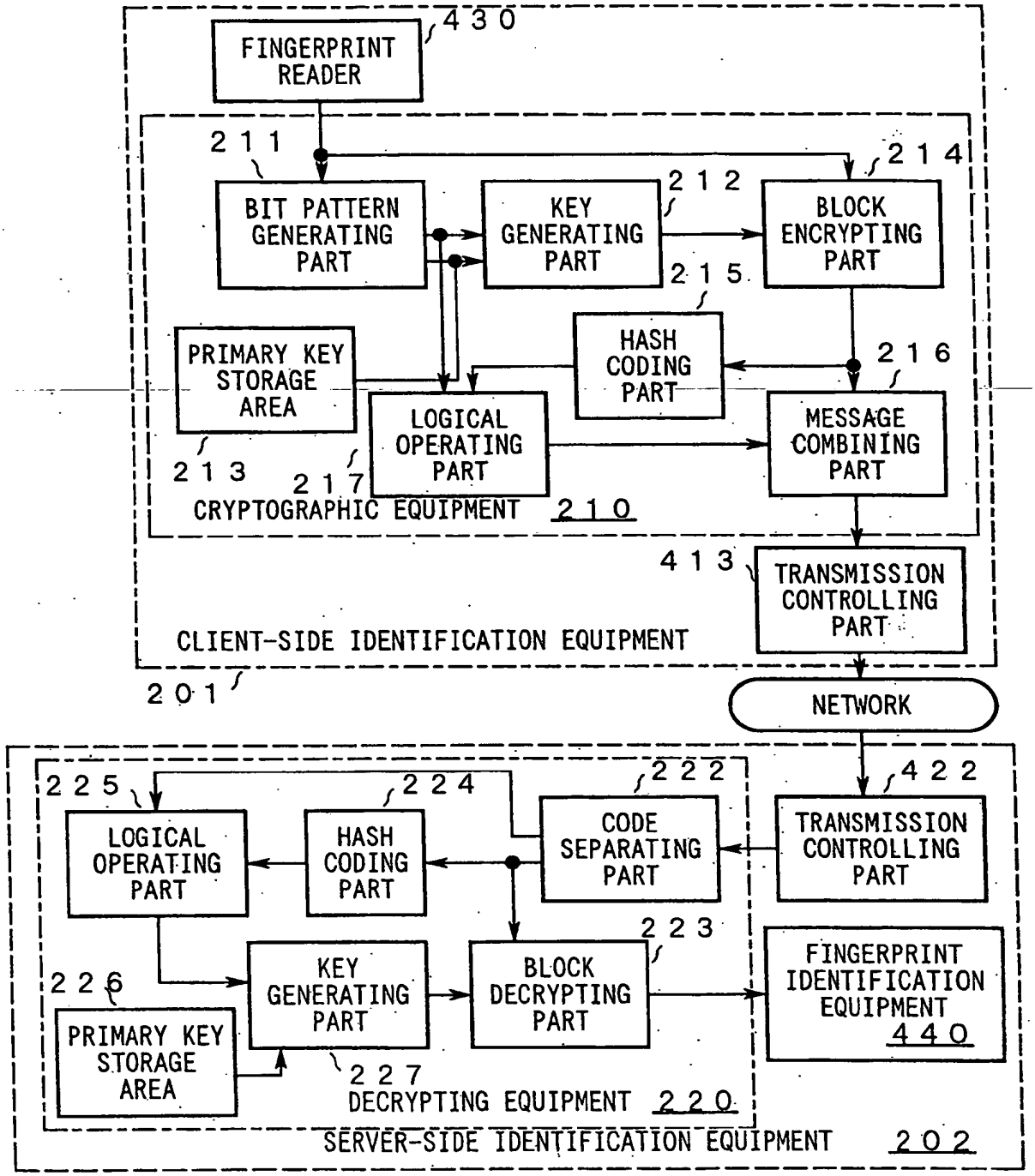

430
FINGERPRINT READER
211
214
212
BIT PATTERN GENERATING PART
KEY GENERATING PART
BLOCK ENCRYPTING PART
215
HASH CODING PART
216
PRIMARY KEY STORAGE AREA
213
217
LOGICAL OPERATING PART
MESSAGE COMBINING PART
CRYPTOGRAPHIC EQUIPMENT 210
413
TRANSMISSION CONTROLLING PART
CLIENT-SIDE IDENTIFICATION EQUIPMENT
201
NETWORK
225
224
222
422
LOGICAL OPERATING PART
HASH CODING PART
CODE SEPARATING PART
TRANSMISSION CONTROLLING PART
223
226
KEY GENERATING PART
BLOCK DECRYPTING PART
FINGERPRINT IDENTIFICATION EQUIPMENT 440
PRIMARY KEY STORAGE AREA
227
DECRYPTING EQUIPMENT 220
SERVER-SIDE IDENTIFICATION EQUIPMENT 202

Fig. 9

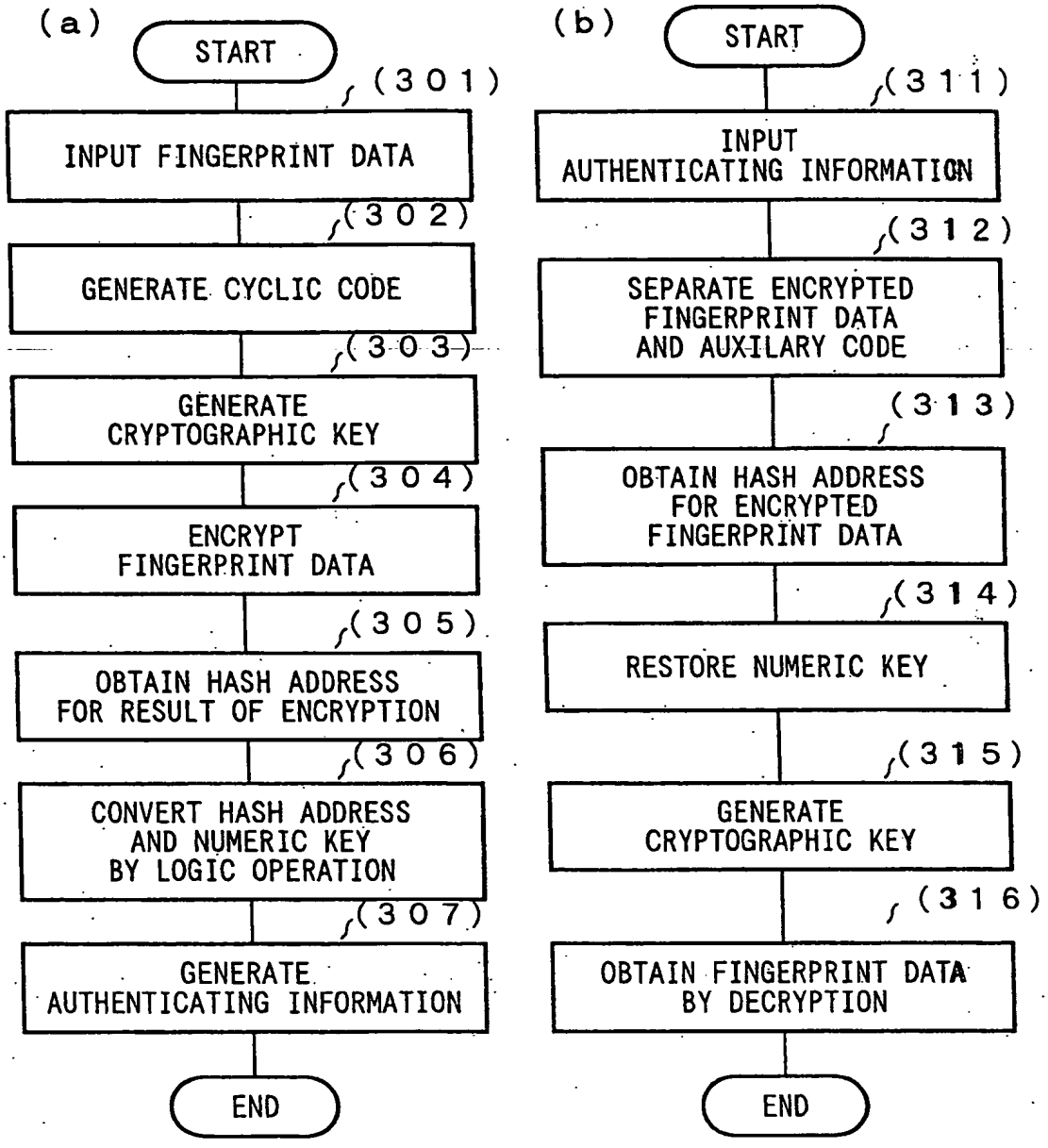
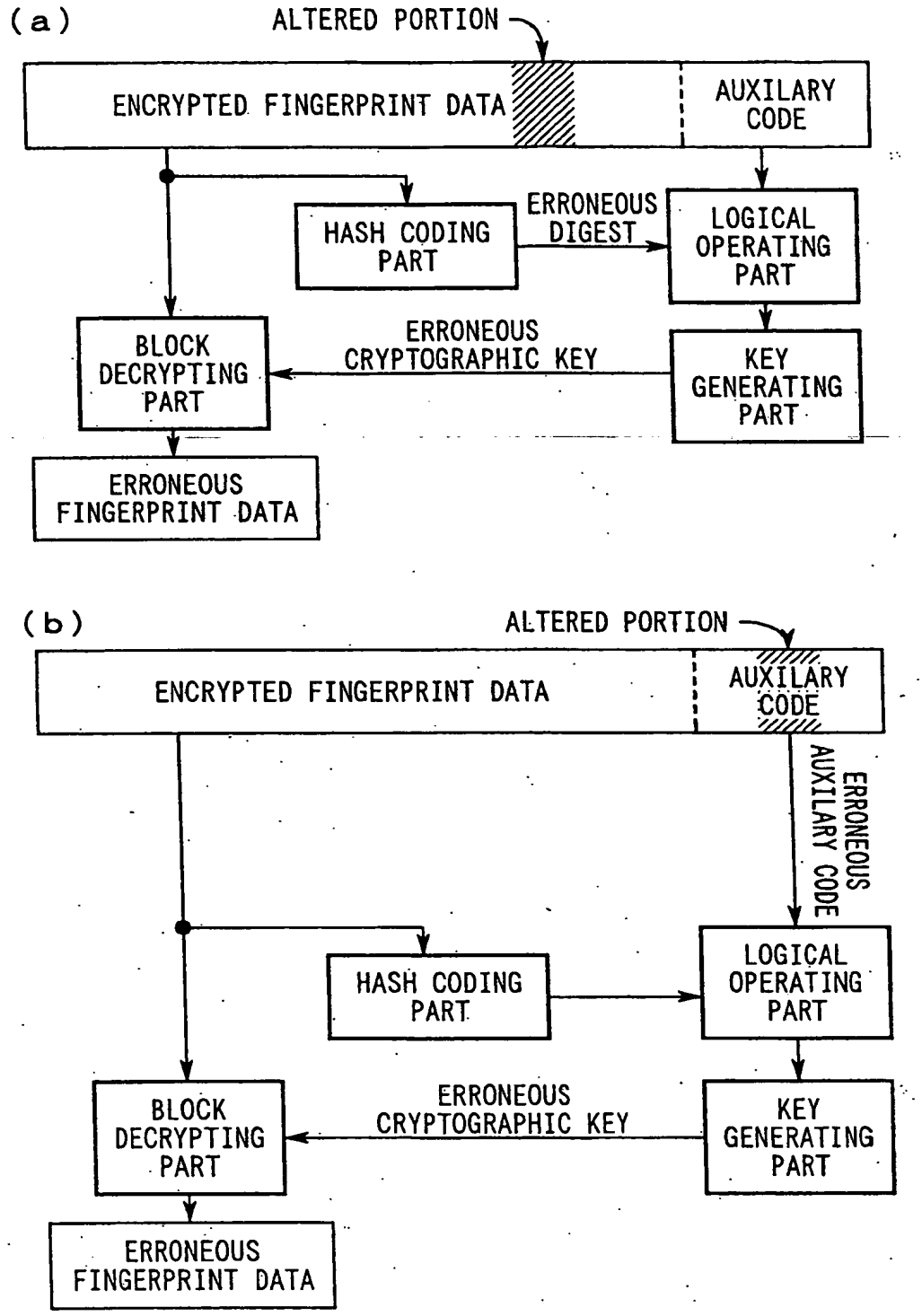

(a)
START
(301)
INPUT FINGERPRINT DATA
(302)
GENERATE CYCLIC CODE
(303)
GENERATE CRYPTOGRAPHIC KEY
(304)
ENCRYPT FINGERPRINT DATA
(305)
OBTAIN HASH ADDRESS FOR RESULT OF ENCRYPTION
(306)
CONVERT HASH ADDRESS AND NUMERIC KEY BY LOGIC OPERATION
(307)
GENERATE AUTHENTICATING INFORMATION
END
(b)
START
(311)
INPUT AUTHENTICATING INFORMATION
(312)
SEPARATE ENCRYPTED FINGERPRINT DATA AND AUXILARY CODE
(313)
OBTAIN HASH ADDRESS FOR ENCRYPTED FINGERPRINT DATA
(314)
RESTORE NUMERIC KEY
(315)
GENERATE CRYPTOGRAPHIC KEY
(316)
OBTAIN FINGERPRINT DATA BY DECRYPTION
END

Fig. 10


(a)
ALTERED PORTION
ENCRYPTED FINGERPRINT DATA
AUXILARY CODE
HASH CODING PART
ERRONEOUS DIGEST
LOGICAL OPERATING PART
BLOCK DECRYPTING PART
ERRONEOUS CRYPTOGRAPHIC KEY
KEY GENERATING PART
ERRONEOUS FINGERPRINT DATA
(b)
ALTERED PORTION
ENCRYPTED FINGERPRINT DATA
AUXILARY CODE
ERRONEOUS AUXILARY CODE
HASH CODING PART
LOGICAL OPERATING PART
BLOCK DECRYPTING PART
ERRONEOUS CRYPTOGRAPHIC KEY
KEY GENERATING PART
ERRONEOUS FINGERPRINT DATA